Commutative Algebra

Swayam Chube

Last Updated: January 22, 2026

§1 Valuation Rings

Definition 1.1. An integral domain R with field of fractions K is said to be a *valuation ring* if for every $x \in K^\times$, $x \in R$ or $x^{-1} \in R$. We also say that R is a valuation ring of K.

Proposition 1.2. Let R be a valuation ring of K. The R-submodules of K are totally ordered with respect to inclusion.

Proof. Let I and J be distinct R-submodules of K. If $I \setminus J \neq \emptyset$, pick $x \in I \setminus J$. For any $0 \neq y \in J$, one of xy^{-1} or $x^{-1}y$ must belong to R. If $xy^{-1} \in R$, then $x = y \cdot (xy^{-1}) \in J$, which is absurd. Thus $x^{-1}y \in R$, so that $y = x \cdot (x^{-1}y) \in I$, and hence, $J \subseteq I$. Argue similarly for the case $J \setminus I \neq \emptyset$. ■

Corollary 1.3. A valuation ring is local.

Proposition 1.4. The following are equivalent for a ring R:

(1) R is a valuation ring.

(2) R is a local Bézout domain.

Proof. (1) $\implies$ (2) follows immediately from Proposition 1.2, since any finitely generated ideal in R can be written as $a_1R + \cdots + a_nR$ for some $a_1, \dots, a_n \in R$.

(2) $\implies$ (1): We must show that for every $x \in K^\times$, either $x \in R$ or $x^{-1} \in R$. Choose $f, g \in R$ such that $x = \frac{f}{g}$, and let $(h) = (f, g)$ as ideals in R. We can find $a, b \in R$ such that $f = ah$ and $g = bh$, and can find $c, d \in R$ such that $h = cf + dg$. Since R is a domain and $h \neq 0$, it follows that $ac + bd = 1$. Therefore, either a or b must be a unit in R, so that either $x \in R$ or $x^{-1} \in R$, thereby completing the proof. ■

Proposition 1.5. A valuation ring is integrally closed.

Proof. Let $(R, \mathfrak{m})$ be a valuation ring with fraction field K. If $x \in K \setminus R$ is integral over R, then there is a non-trivial relation of the form
$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$
with $a_i \in R$ for $0 \leqslant i \leqslant n-1$. Multiplying out by $x^{-n} \in \mathfrak{m}$, we have that $1 \in \mathfrak{m}$, a contradiction. Thus R is integrally closed. ■

Remark 1.6. We note here that given a field K, a valuation ring of K is determined by its maximal ideal. Indeed, if $(R, \mathfrak{m})$ is a valuation ring of K, then we can write
$$K \setminus R = \left\{x^{-1} : x \in \mathfrak{m} \setminus \{0\}\right\}.$$

Further note that if R is a valuation ring of K, then any subring of K containing R is also a valuationg ring of K.

THEOREM 1.7. Let R be a valuation ring of K and R' a subring of K containing R. Let $\mathfrak{m}$ denote the maximal ideal of R, $\mathfrak{p}$ the maximal ideal of R', and suppose that $R \neq R'$. Then

(1) $\mathfrak{p} \subsetneq \mathfrak{m} \subseteq R \subseteq R'$.

(2) $\mathfrak{p}$ is a prime ideal of R and $R' = R_{\mathfrak{p}}$.

(3) $R/\mathfrak{p}$ is a valuation ring of the field $R'/\mathfrak{p}$.

(4) Given a valuation ring $\overline{S}$ of the field $R/\mathfrak{m}$, let S denote its preimage in R. Then S is a valuation ring of K and is called the *composite* of R and $\overline{S}$.

Proof. (1) Let $0 \neq x \in \mathfrak{p}$. Then $x^{-1} \in K \setminus R' \subseteq K \setminus R$, so that $x \in \mathfrak{m}$. Thus $\mathfrak{p} \subseteq \mathfrak{m}$. In light of Remark 1.6, $\mathfrak{p} \neq \mathfrak{m}$.

(2) Since $R/\mathfrak{p} \hookrightarrow R'/\mathfrak{p}$ as a subring, it is clear that $\mathfrak{p}$ is a prime ideal in R. Further, since every element of $R \setminus \mathfrak{p}$ is invertible in R', $R \subseteq R_{\mathfrak{p}} \subseteq R'$. Note that $\mathfrak{p}$ is an ideal in $R_{\mathfrak{p}}$, and hence, $\mathfrak{p}R_{\mathfrak{p}} = \mathfrak{p}$, so that $R_{\mathfrak{p}} = R'$ due to (1).

(3) Straightforward.

(4) Let $\pi : R \to R/\mathfrak{m}$ denote the projection map. Note that $\mathfrak{m} \subseteq S$ and $S/\mathfrak{m} = \overline{S}$. If $x \in R \setminus S$, then $\pi(x) \notin \overline{S}$, and therefore, $\pi(x^{-1}) = \pi(x)^{-1} \in S$. Hence $x^{-1} \in S$. On the other hand, if $x \in K \setminus R$, then $x^{-1} \in \mathfrak{m} \subseteq S$. This shows that S is a valuation ring of K. ∎

THEOREM 1.8. Let K be a field, $A \subseteq K$ a subring, and $\mathfrak{p}$ a prime ideal of A. Then there exists a valuation ring $(R, \mathfrak{m})$ of K such that $A \subseteq R$, and $\mathfrak{m} \cap A = \mathfrak{p}$.

Proof. First, replacing A by $A_{\mathfrak{p}}$, we may assume that A is a local ring with maximal ideal $\mathfrak{p}$. Let $\mathscr{F}$ denote the set of all subrings B of K containing A such that $1 \notin \mathfrak{p}B$. Clearly, every ascending chain in $\mathscr{F}$ has an upper bound given by the union of all elements of the chain. Using Zorn's lemma, choose a maximal element R in $\mathscr{F}$. First, we contend that R is a local ring. Indeed, since $1 \notin \mathfrak{p}R$, there is a maximal ideal $\mathfrak{m}$ of R containing $\mathfrak{p}R$. Note that $R_{\mathfrak{m}} \in \mathscr{F}$, so that $R = R_{\mathfrak{m}}$ in view of the maximality of R. Next, $\mathfrak{m} \cap A$ is a proper ideal containing $\mathfrak{p}$, which, due to the maximality of $\mathfrak{p}$ must be equal to $\mathfrak{p}$.

It remains to show that R is a valuation ring of K. Suppose $x \in K$ is such that $x, x^{-1} \notin R$. Then $R \subsetneq R[x]$, and hence $1 \in \mathfrak{p}R[x]$, i.e., there is a polynomial relation

$$1 = a_0 + a_1 x + \cdots + a_n x^n$$

with $a_i \in \mathfrak{p}R \subseteq \mathfrak{m}$ for $0 \leqslant i \leqslant n$. Multiplying by $(1 - a_0)^{-1} \in R$, one obtains a relation of the form

$$1 = b_1 x + \cdots + b_n x^n$$

with $b_i \in \mathfrak{p}R$ for $1 \leqslant i \leqslant n$. Choose one such relation with the smallest possible value of n. Arguing similarly for x^{-1}, choose a relation

$$1 = c_1 x^{-1} + \cdots + c_m x^{-m}$$

with the smallest possible value of m. If $n \geqslant m$, then multiply the second equation by $b_n x^n$ and subtract from the first to obtain a non-trivial relation of smaller degree than n, a contradiction. On the other hand, if $m > n$, then multiply the first relation by $c_m x^{-m}$ and subtract from the second to obtain a non-trivial relation of smaller degree than m, a contradiction again. Thus $x \in R$ or $x^{-1} \in R$, i.e., R is a valuation ring of K. ∎

THEOREM 1.9. Let K be a field, $A \subseteq K$ a subring, and B the integral closure of A in K. Then B is equal to the intersection of all valuation rings of K containing A.

Proof. Let C denote the intersection of all valuation rings of R containing A. In view of Proposition 1.5, B is contained in every such valuation ring, so that $B \subseteq C$. Now let $x \in K$ be non-integral over A and set $y = x^{-1}$. Note that $1 \notin yA[y]$, else x would be integral over A. Let $\mathfrak{p}$ be a maximal ideal of $A[y]$ containing $yA[y]$, and using Theorem 1.8, choose a valuation ring $(R, \mathfrak{m})$ of K containing $A[y]$ such that $\mathfrak{m} \cap A[y] = \mathfrak{p}$. In particular, $y \in \mathfrak{m}$, so that $x \notin R$. Thus $x \notin C$, as desired. ■

§§ Valuations

DEFINITION 1.10. An abelian group Γ together with a total order relation $\leqq$ is said to be *ordered* if for all $x, y \in \Gamma$ with $x \leqq y$, $x + z \leqq y + z$ for all $z \in \Gamma$.

Let K be a field. A *valuation* on K is a map $v : K \to \Gamma \cup \{\infty\}$ satisfying:

(i) $v(x) = \infty$ if and only if $x = 0$,

(ii) $v(xy) = v(x) + v(y)$[1], and

(iii) $v(x + y) \geqslant \min\{v(x), v(y)\}$

for all $x, y \in K$.

Corresponding to a valuation v on K, we can define

$$R_v = \{x \in K : v(x) \geqslant 0\} \quad \text{and} \quad \mathfrak{m}_v = \{x \in K : v(x) > 0\}.$$

It is not hard to see that $(R_v, \mathfrak{m}_v)$ is a valuation ring of K. Conversely, we show that every valuation ring arises this way. Let

$$\Gamma = \left\{xR : x \in K^\times\right\}.$$

This is a group under the operation

$$(xR) \cdot (yR) = xyR$$

with neutral element R. Further, note that Γ is an ordered abelian group when equipped with the total ordering

$$xR \leqq yR \iff xR \supseteq yR,$$

where we are implicitly invoking Proposition 1.2. Define $v : K \to \Gamma \cup \{\infty\}$ sending

$$v(x) = \begin{cases} xR & x \neq 0 \\ \infty & x = 0. \end{cases}$$

Note that $xR \geqq R$ if and only if $xR \subseteq R$, that is, if $x \in R$. Hence, $R_v = R$ and $\mathfrak{m}_v = \mathfrak{m}$. This shows that every valuation ring arises from a valuation of K.

DEFINITION 1.11. The *value group* of a valuation ring $(R, \mathfrak{m})$ of K is $v(K^\times)$, where v is a valuation of K such that $(R_v, \mathfrak{m}_v) = (R, \mathfrak{m})$.

To see that the value group is well-defined:

[1] so that v is a group homomorphism when restricted to $K^\times$

PROPOSITION 1.12. If v and v' are two valuations of K corresponding to the same valuation ring R and having value groups H and H' respectively, then there is an order-isomorphism $\varphi\colon H \to H'$ such that $v' = \varphi \circ v$.

Proof. Let $v\colon K^\times \to \Gamma$ and $v'\colon K^\times \to \Gamma'$ be the two valuations. Define $\varphi\colon H \to H'$ by $\varphi(v(x)) = v'(x)$ for all $x \in K^\times$. We must show that φ is well-defined. Indeed, if $x, y \in K^\times$ are such that $v(x) = v(y)$, then $x^{-1}y$ is a unit in R, so that $v'(x^{-1}y) = 0$, i.e., $v'(x) = v'(y)$. That φ is a group homomorphism is clear. The surjectivity of φ is immediate from the fact that $v' = \varphi \circ v$. As for injectivity, if $\varphi(v(x)) = 0$, then $v'(x) = 0$, and hence x is a unit in R, so that $v(x) = 0$. Finally, if $v(x) \leqq v(y)$, then $v(x^{-1}y) \geqq 0$, so that $x^{-1}y \in R$, i.e., $v'(x^{-1}y) \geqq 0$, that is, $v'(y) \geqq v'(x)$. Thus φ is an order-isomorphism. ∎

§2 Discrete Valuation Rings and Dedekind Domains

§§ Discrete Valuation Rings

DEFINITION 2.1. A valuation ring with value group order-isomorphic to $\mathbb{Z}$ is called a *discrete valuation ring (DVR)*.

THEOREM 2.2. Let R be a valuation ring. Then the following are equivalent:

(1) R is a DVR.

(2) R is a PID.

(3) R is Noetherian.

Proof. Let K be the field of fractions of R and $\mathfrak{m}$ its maximal ideal.
(1) $\Longrightarrow$ (2) Let $v\colon K^\times \to \mathbb{Z}$ be a surjective valuation corresponding to R. Let $t \in \mathfrak{m}$ be such that $v(t) = 1$. For $0 \neq x \in \mathfrak{m}$, $v(x) = n > 0$ for some positive integer n. Then $v(x/t^n) = 0$, i.e., $x = ut^n$ for some unit $u \in R^\times$. In particular, this shows that $\mathfrak{m} = tR$. Now let $0 \neq I$ be a proper ideal in R, and let

$$n = \min\{v(a)\colon 0 \neq a \in I\}.$$

Clearly n is a positive integer since I is proper. Let $x \in I$ with $v(x) = n$. Then $xR \subseteq I$, and for every $y \in I$, $v(y/x) \geqslant 0$, so that $y \in xR$. Thus $I = xR$, and R is a PID.
(2) $\Longrightarrow$ (3) is clear.
(3) $\Longrightarrow$ (2) A Noetherian Bézout domain is a PID.
(2) $\Longrightarrow$ (1) Let $t \in \mathfrak{m}$ be such that $\mathfrak{m} = tR$. Recall that a PID is a UFD, and let v denote the t-adic valuation on K. It is not hard to see that R is the valuation ring corresponding to v. ∎

DEFINITION 2.3. If R is a DVR with maximal ideal $\mathfrak{m}$, then any element $t \in \mathfrak{m}$ such that $\mathfrak{m} = tR$ is said to be a *uniformizer* or a *uniformizing element* of R.

REMARK 2.4. We note here that a valuation ring whose maximal ideal is principal need not necessarily be a DVR. Indeed, let K be a field, $(R, \mathfrak{m}_R)$ a DVR of K, set $k = R/\mathfrak{m}_R$, and suppose $\mathfrak{R}$ is a DVR of k. Let S denote the composite of R and $\mathfrak{R}$. We contend that S is our desired counterexample.

Let $f \in \mathfrak{m}_R$ be a uniformizer of R, $g \in S$ such that $\overline{g} = g + \mathfrak{m}_R$ is a uniformizer of $\mathfrak{R}$. Then $\mathfrak{m}_S = \mathfrak{m}_R + gS$. Further, since $g \notin \mathfrak{m}_R$, it is a unit in R, so that $g^{-1} \in R$. Hence, for any element $h \in \mathfrak{m}_R$, we can write $h = g \cdot (g^{-1}h)$, so that $\mathfrak{m}_R \subseteq gS$. Hence $\mathfrak{m}_S = gS$ is principal.

Next, we show that S is not Noetherian. Indeed, consider the ascending chain of ideals in S:

$$(f) \subseteq (f, fg^{-1}) \subseteq (f, fg^{-1}, fg^{-2}) \subseteq \cdots.$$

We claim that all the above inclusions are proper. Indeed, if $fg^{-(n+1)} \in (f, fg^{-1}, \ldots, fg^{-n})$ for some $n \geqslant 0$, then there exist $a_0, \ldots a_n \in S$ such that

$$fg^{-(n+1)} = a_0 f + a_1 fg^{-1} + \cdots + a_n fg^{-n}.$$

Multiplying out by $f^{-1}g^{n+1}$, we obtain

$$a_0 g^{n+1} + \cdots + a_n g = 1,$$

which is absurd, since $1 \notin \mathfrak{m}_S = gS$, thereby completing the proof.

THEOREM 2.5. Let R be a ring. The following conditions are equivalent:

(1) R is a DVR.

(2) R is a local PID but not a field.

(3) R is a Noetherian local ring, $\dim R > 0$, and the maximal ideal of R is principal.

(4) R is a one-dimensional normal Noetherian local domain.

Proof. (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) is clear.

(3) $\Longrightarrow$ (1) Let $\mathfrak{m} = tR$ denote the maximal ideal of R. Due to Krull's intersection theorem,

$$\bigcap_{n=1}^{\infty} \mathfrak{m}^n = (0).$$

Hence, for every $0 \neq x \in R$, there is a non-negative integer n such that $x \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$. Set $v(x) = n$. Now if $x, y \in R \setminus \{0\}$ are such that $v(x) = n$ and $v(y) = m$, then we can find units $u, v \in R^\times$ such that $x = t^n u$ and $y = t^m v$. This shows that $xy = t^{m+n}uv \neq 0$, so that R is an integral domain and $v(xy) = v(x) + v(y)$. Let K denote the fraction field of R, and set

$$v\left(\frac{a}{b}\right) = v(a) - v(b)$$

for all $a, b \in R \setminus \{0\}$. This is clearly well-defined, and defines a valuation on K whose value group is $\mathbb{Z}$ and corresponding valuation ring is R. Hence R is a DVR.

(1) $\Longrightarrow$ (4) Recall that in a DVR the only ideals are (0) and powers of the maximal ideal. Thus the only prime ideals are (0) and $\mathfrak{m}$, so that $\dim R = 1$. That R is Noetherian follows from it being a PID, and finally recall that every valuation ring is normal.

(4) $\Longrightarrow$ (3) Let $\mathfrak{m}$ denote the maximal ideal of R. Due to Nakayama's lemma and the fact that $\dim R = 1$, $\mathfrak{m} \neq \mathfrak{m}^2$. Choose $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. We shall show that $\mathfrak{m} = xR$. Note that $\mathfrak{m} \in \mathrm{Ass}_R(R/xR)$, so that there exists $y \in R \setminus xR$ such that $(xR : y) = \mathfrak{m}$. Set $a = yx^{-1} \in K := \mathrm{Frac}(R)$. Note that $a \notin R$ lest $y \in xR$. Set

$$\mathfrak{m}^{-1} := \{\alpha \in K \colon \alpha\mathfrak{m} \subseteq R\}.$$

Note that $\mathfrak{m}^{-1}$ is an R-submodule of K, and further, by construction,

$$\mathfrak{m}\mathfrak{m}^{-1} := \left\{R\text{-submodule of } K \text{ generated by } x_i y_i : x_i \in \mathfrak{m},\ y_i \in \mathfrak{m}^{-1}\right\} \subseteq R \quad \text{and} \quad R \subseteq \mathfrak{m}^{-1}.$$

In particular, we have the inclusions $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{m}^{-1} \subseteq R$. Hence, $\mathfrak{m}\mathfrak{m}^{-1} \in \{\mathfrak{m}, R\}$. If $\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{m}$, then $a\mathfrak{m} \subseteq \mathfrak{m}$. Since $\mathfrak{m}$ is a finite R-module, due to Nakayama's lemma, a must be integral over R, but since R is normal, $a \in R$, a contradiction. Thus $\mathfrak{m}^{-1}\mathfrak{m} = R$. Next, note that $x\mathfrak{m}^{-1} \subseteq R$. If $x\mathfrak{m}^{-1} \subseteq \mathfrak{m}$, then

$$xR = x\mathfrak{m}^{-1}\mathfrak{m} \subseteq \mathfrak{m}^2,$$

a contradiction. Hence, $x\mathfrak{m}^{-1} = R$, so that

$$xR = x\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{m},$$

thereby completing the proof. ■

§§ Fractional Ideals and Dedekind domains

Definition 2.6. Let R be an integral domain with fraction field K. An R-submodule I of K is said to be a *fractional ideal* if there is a non-zero $\alpha \in R$ such that $\alpha I \subseteq R$.

The standard operations on ideals readily generalize to operations on fractional ideals. Indeed, if I and J are fractional ideals, define

$$\begin{aligned} I + J &= \{x + y : x \in I,\ y \in J\} \\ IJ &= \{R\text{-submodule generated by } x_i y_i : x_i \in I,\ y_i \in J\}. \end{aligned}$$

Clearly, both $I + J$ and IJ are fractional ideals of R. Further, if $S \subseteq R$ is a multiplicative set, then

$$S^{-1}I = \left\{\frac{x}{s} : x \in I,\ s \in S\right\}$$

is a fractional ideal of $S^{-1}R$.

Lemma 2.7. Let R be an integral domain, M and N R-submodules of $K = \mathrm{Frac}(R)$. If N is finitely generated, then

$$S^{-1}(M : N) = \left(S^{-1}M : S^{-1}N\right).$$

Proof. Clearly $S^{-1}(M : N) \subseteq \left(S^{-1}M : S^{-1}N\right)$. Since N is finitely generated, we can write $N = a_1R + \cdots + a_nR$ for some $a_1, \ldots, a_n \in K$. If $x \in \left(S^{-1}M : S^{-1}N\right)$, then for all $1 \leqslant i \leqslant n$, $xa_i \in S^{-1}M$. Therefore, there exist $c_i \in S$ such that $c_i x a_i \in M$, whence $c_i x \in (M : N)$, so that $x \in S^{-1}(M : N)$. ∎

Definition 2.8. An R-submodule I of K is said to be *invertible* if there exists an R-submodule J of K such that $IJ = R$.

Proposition 2.9. An invertible R-submodule of K must be a finite R-module.

Proof. Let I be an invertible fractional ideal of R and J an R-submodule of K such that $IJ = R$. Then we can find $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n \in J$ such that

$$1 = a_1 b_1 + \cdots + a_n b_n.$$

For each $x \in I$, we can write

$$x = (xb_1)a_1 + \cdots + (xb_n)a_n,$$

and note that $xb_i \in R$ for $1 \leqslant i \leqslant n$. It follows that $I = a_1R + \cdots + a_nR$. ∎

Corollary 2.10. Every invertible R-submodule of K is a fractional ideal.

Remark 2.11. Suppose I is an invertible fractional ideal of R, and set

$$I^{-1} := \{\alpha \in K : \alpha I \subseteq R\}.$$

This is clearly an R-submodule of K. Further, note that $II^{-1} \subseteq R$, so that

$$I^{-1} = JII^{-1} \subseteq J.$$

But since $JI \subseteq R$, we clearly have $J \subseteq I^{-1}$. This shows that $J = I^{-1}$.

Theorem 2.12. Let R be an integral domain and I an R-submodule of K. The following are equivalent:

(1) I is an invertible fractional ideal.

(2) I is a projective R-module.

(3) I is a finite R-module, and for each maximal ideal $\mathfrak{m}$ of R, the fractional ideal $I_{\mathfrak{m}} := IR_{\mathfrak{m}}$ of $R_{\mathfrak{m}}$ is principal.

Proof. (1) $\implies$ (2) Let $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n \in I^{-1}$ be such that $1 = a_1 b_1 + \cdots + a_n b_n$. As we have seen in the proof of Proposition 2.9, $I = a_1 R + \cdots + a_n R$. Let $\pi : F := \bigoplus_{i=1}^{n} Re_i \to I$ be the map sending $e_i \mapsto a_i$. Define $\sigma : I \to F$ by

$$\sigma(x) = (xb_1)e_1 + \cdots + (xb_n)e_n.$$

It is then clear that $\pi \circ \sigma = \mathbf{id}_I$, so that I is projective.

(2) $\implies$ (1) There is a free module $F = \bigoplus_i Re_i$ and an epimorphism $\pi : F \to I$ which splits through an R-linear map $\sigma : I \to F$. Let $a_i = \pi(e_i)$ and $\lambda_i = \pi_i \circ \sigma : I \to R$. Note that every R-linear map $I \to R$ is multiplication by some element of K. Say $\lambda_i(x) = b_i x$ for all $x \in I$. Note that $b_i \in I^{-1}$ for all i. Then

$$\pi(\sigma(x)) = \sum_i a_i b_i x \implies \sum_i a_i b_i = 1.$$

Set J denote the R-submodule of K generated by the b_i's. Then $R \subseteq IJ \subseteq R$, and hence I is an invertible fractional ideal.

(1) $\implies$ (3) That I is a finite R-module is the content of Proposition 2.9. Further,

$$R_{\mathfrak{m}} = \left(II^{-1}\right)_{\mathfrak{m}} = I_{\mathfrak{m}} \left(I^{-1}\right)_{\mathfrak{m}},$$

so that $I_{\mathfrak{m}}$ is an invertible fractional ideal of $R_{\mathfrak{m}}$. Due to (2), $I_{\mathfrak{m}}$ is a projective $R_{\mathfrak{m}}$-module. But since any two elements of K are $R_{\mathfrak{m}}$-linearly dependent, $I_{\mathfrak{m}}$ must be principal.

(3) $\implies$ (1) Note that for every maximal ideal $\mathfrak{m}$ of R,

$$\left(I^{-1}\right)_{\mathfrak{m}} = (R : I)_{\mathfrak{m}} = (R_{\mathfrak{m}} : I_{\mathfrak{m}}) = (I_{\mathfrak{m}})^{-1}.$$

If $II^{-1} \subsetneq R$, then there is a maximal ideal $\mathfrak{m}$ containing II^{-1}, so that

$$\mathfrak{m}R_{\mathfrak{m}} \supseteq \left(II^{-1}\right)_{\mathfrak{m}} = I_{\mathfrak{m}} \left(I^{-1}\right)_{\mathfrak{m}} = I_{\mathfrak{m}} I_{\mathfrak{m}}^{-1} = R_{\mathfrak{m}},$$

a contradiction. This completes the proof. ■

THEOREM 2.13. Let R be a Noetherian domain, and $\mathfrak{p}$ a non-zero prime ideal of R. If $\mathfrak{p}$ is invertible, then $\operatorname{ht}\mathfrak{p} = 1$ and $R_{\mathfrak{p}}$ is a DVR.

Proof. Since $\mathfrak{p}$ is invertible, due to Theorem 2.12, $\mathfrak{p}R_{\mathfrak{p}}$ is a principal ideal. Since $\dim R_{\mathfrak{p}} = \operatorname{ht}\mathfrak{p} > 0$, it follows from Theorem 2.5 that $R_{\mathfrak{p}}$ is a DVR, and hence $\operatorname{ht}\mathfrak{p} = \dim R_{\mathfrak{p}} = 1$. ■

THEOREM 2.14. Let R be a normal Noetherian domain. Then

(1) all prime divisors of a non-zero principal ideal have height 1.

(2) $R = \bigcap_{\operatorname{ht}\mathfrak{p}=1} R_{\mathfrak{p}}$.

Proof. (1) This follows from Krull's Hauptidealsatz.

(2) Suppose $\dfrac{a}{b} \in \bigcap_{\operatorname{ht}\mathfrak{p}=1} R_{\mathfrak{p}}$ with $b \neq 0$. We shall show that $a \in bR$. If b is a unit in R, then there is nothing to prove. If b is not a unit in R, consider the primary decomposition

$$bR = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$$

with corresponding associated primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Due to (1), we know that $\operatorname{ht}\mathfrak{p}_i = 1$ for all i, so that there are no embedded associated primes. Localising at $\mathfrak{p}_i$ and contracting back to R, we have

$$\mathfrak{q}_i = bR_{\mathfrak{p}} \cap R \ni a.$$

Therefore,

$$a \in \bigcap_{i=1}^{r} \mathfrak{q}_i = bR,$$

as desired. ■

Porism 2.15. Let R be a Noetherian domain. If all associated primes of a non-zero principal ideal have height 1, then

$$R = \bigcap_{\operatorname{ht}\mathfrak{p}=1} R_{\mathfrak{p}}.$$

Corollary 2.16. Let R be a Noetherian domain. Then R is normal if and only if the following two conditions are satisfied:

(i) for every height 1 prime $\mathfrak{p}$, $R_{\mathfrak{p}}$ is a DVR; and

(ii) all associated primes of a non-zero principal ideal of R have height 1.

Proof. Necessity is the content of Theorem 2.14. For sufficiency, note that due to Porism 2.15, $R = \bigcap_{\operatorname{ht}\mathfrak{p}=1} R_{\mathfrak{p}}$. But since each $R_{\mathfrak{p}}$ is a DVR, it is normal, so that R is normal. ■

Definition 2.17. An integral domain for which every ideal is invertible is called a *Dedekind domain*.

Theorem 2.18. For an integral domain R, the following conditions are equivalent:

(1) R is a Dedekind domain.

(2) R is either a field or a one-dimensional Noetherian normal domain.

(3) every non-zero ideal of R can be written as a product of a finite number of prime ideals.

Proof. (1) $\Longrightarrow$ (2) Suppose R is a field. Since every ideal is invertible, it is finitely generated, so that R is Noetherian. If $\mathfrak{p}$ is a non-zero prime ideal of R, then due to Theorem 2.12, $\mathfrak{p}R_{\mathfrak{p}}$ is a principal ideal. Due to Theorem 2.5, $R_{\mathfrak{p}}$ is a DVR and $\operatorname{ht}\mathfrak{p} = 1$. Since R is not a field, every prime ideal is a maximal ideal, and hence, we can write

$$R = \bigcap_{0 \neq \mathfrak{p} \in \operatorname{Spec} R} R_{\mathfrak{p}}.$$

Being the intersection of normal domains, R is also a normal domain.

(2) $\Longrightarrow$ (1) Let I be an ideal of R. We shall show that I is invertible. For a maximal ideal $\mathfrak{m}$ of R, note that $R_{\mathfrak{m}}$ is a one-dimensional Noetherian normal local ring, which, due to Theorem 2.5, is a DVR. In particular, $IR_{\mathfrak{m}}$ is a principal ideal. Thus, due to Theorem 2.12, I is invertible.

(1) $\Longrightarrow$ (3) That R is Noetherian follows from (2). We prove (3) by Noetherian induction. Let $\mathscr{F}$ denote the set of all non-zero proper ideals in R that are not products of prime ideals. If $\mathscr{F}$ is

non-empty, using the Noetherian-ness of R, choose a maximal elmeent $I \in \mathscr{F}$. Note that every proper ideal of R properly containing I can be expressed as a product of prime ideals. Let $\mathfrak{m}$ be a maximal ideal containing I. Clearly $I \neq \mathfrak{m}$ else it has a trivial expression as a product of prime ideals. Since $R \subseteq \mathfrak{m}^{-1}$, we have $I \subseteq I\mathfrak{m}^{-1} \subseteq \mathfrak{m}\mathfrak{m}^{-1} = R$. If $I\mathfrak{m}^{-1} = I$, then due to Nakayama's lemma, every element of $\mathfrak{m}^{-1}$ would be integral over R, and therefore must be an element of R due to (2), a contradiction. Thus $I\mathfrak{m}^{-1} \supsetneq I$, so that it can be expressed as a product of prime ideals. Multiplying this expression by $\mathfrak{p}$, we see that I can be expressed as a product of prime ideals too, a contradiction. Thus $\mathscr{F}$ is empty, as desired.

(3) $\implies$ (1) We shall show that every prime ideal in R is invertible. The factorization property would then imply the same for all non-zero ideals of R.

Step 1. Suppose I and J are fractional ideals of R such that $B = IJ$ is an invertible fractional ideal. We shall show that I and J are invertible. First, note that

$$I^{-1}J^{-1}B = I^{-1}J^{-1}JI \subseteq R \implies I^{-1}J^{-1} = I^{-1}J^{-1}BB^{-1} \subseteq B^{-1}.$$

Also, since $B^{-1}IJ = R$, we have the two obvious inclusions $B^{-1}I \subseteq J^{-1}$ and $B^{-1}J \subseteq I^{-1}$. Multiplying these two inclusions, we obtain

$$B^{-1} \subseteq I^{-1}J^{-1} \implies I^{-1}J^{-1} = B^{-1}.$$

Finally, note that

$$R = BB^{-1} = (II^{-1})(JJ^{-1}),$$

so that $II^{-1} = JJ^{-1} = R$, i.e., I and J are invertible.

Step 2. Let $\mathfrak{p}$ be a non-zero prime ideal in R. We shall show that for any ideal I of R properly containing $\mathfrak{p}$, $\mathfrak{p} = I\mathfrak{p}$. To this end, it suffices to show that $\mathfrak{p} \subseteq I\mathfrak{p}$. Let $a \in I \setminus \mathfrak{p}$ and set $J = aR + \mathfrak{p}$. It suffices to show that $\mathfrak{p} \subseteq J\mathfrak{p}$ so that we may replace I by J and continue our analysis. Consider prime decompositions of the two ideals

$$I^2 = \mathfrak{p}_1 \cdots \mathfrak{p}_r \quad \text{and} \quad a^2R + \mathfrak{p} = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Clearly each of the $\mathfrak{q}_i$'s contain $\mathfrak{p}$. Since $I^2 \subseteq \mathfrak{p}_i$, we have $I \subseteq \mathfrak{p}_i$, so that $\mathfrak{p} \subseteq \mathfrak{p}_i$. Let $\overline{R} := R/\mathfrak{p}$, and for each $x \in R$, let $\overline{x}$ denote its image in $\overline{R}$. Note that $\overline{R}$ is an integral domain with the factorization property (3), and in $\overline{R}$, we have the decompositions

$$\overline{\mathfrak{p}}_1 \cdots \overline{\mathfrak{p}}_r = \overline{a}^2\overline{R} = \overline{\mathfrak{q}}_1 \cdots \overline{\mathfrak{q}}_s.$$

Since $\overline{a}^2\overline{R}$ is an invertible ideal of $\overline{R}$, due to Step 1, all the $\overline{\mathfrak{p}}_i$'s and the $\overline{\mathfrak{q}}_j$'s are invertible ideals of $\overline{R}$. Now let $\overline{\mathfrak{p}}_1$ be a minimal element of the set $\{\overline{\mathfrak{p}}_1, \ldots, \overline{\mathfrak{p}}_r\}$. Since $\overline{\mathfrak{p}}_1 \supseteq \overline{\mathfrak{q}}_1 \cdots \overline{\mathfrak{q}}_s$, using Prime Avoidance, $\overline{\mathfrak{p}}_1$ must contain one of the $\overline{\mathfrak{q}}_i$'s, say without loss of generality, $\overline{\mathfrak{q}}_1$. An analogous argument would give that $\overline{\mathfrak{q}}_1$ must contain some $\overline{\mathfrak{p}}_j$, which, due to the minimality of $\overline{\mathfrak{p}}_1$ must be equal to $\overline{\mathfrak{p}}_1$ – that is, $\overline{\mathfrak{p}}_1 = \overline{\mathfrak{q}}_1$. Since these ideals are invertible, multiplying with their inverses, we are left with

$$\overline{\mathfrak{p}}_2 \cdots \overline{\mathfrak{p}}_r = \overline{\mathfrak{q}}_2 \cdots \overline{\mathfrak{q}}_s.$$

Continuing in this way, we obtain $r = s$ and $\overline{\mathfrak{p}}_i = \overline{\mathfrak{q}}_i$ for $1 \leqslant i \leqslant r$. In particular, $\mathfrak{p}_i = \mathfrak{q}_i$ for $1 \leqslant i \leqslant r$, so that

$$a^2R + \mathfrak{p} = (aR + \mathfrak{p})^2 = a^2R + a\mathfrak{p} + \mathfrak{p}^2.$$

Hence, every $x \in \mathfrak{p}$ can be written as

$$x = a^2y + az + w \qquad \text{where} \quad y \in R,\ z \in \mathfrak{p},\ \text{and}\ w \in \mathfrak{p}^2.$$

Thus $a^2 y \in \mathfrak{p}$ – but since $a \notin \mathfrak{p}$, $y \in \mathfrak{p}$. This gives

$$\mathfrak{p} \subseteq a\mathfrak{p} + \mathfrak{p}^2 = I\mathfrak{p},$$

as desired.
Step 3. Let $0 \neq a \in R$. Then in the factorization $bR = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, all the $\mathfrak{p}_i$'s are maximal. Indeed, if I is any ideal properly containing $\mathfrak{p}_i$, then due to Step 2, $\mathfrak{p}_i = I\mathfrak{p}_i$. As we have already argued, every $\mathfrak{p}_i$ is invertible, so that $I = R$.
Step 4. Let $\mathfrak{p}$ be a non-zero prime ideal in R, and let $0 \neq a \in R$. If $aR = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, then due to Step 3, each $\mathfrak{p}_i$ is maximal. Since $\mathfrak{p} \supseteq aR$, there is an index i such that $\mathfrak{p}_i \subseteq \mathfrak{p}$. The maximality of $\mathfrak{p}_i$ forces $\mathfrak{p}_i = \mathfrak{p}$. In particular, $\mathfrak{p}$ is invertible, thereby completing the proof. ■